مضى 2444 يوماً منذ إعلان دولة الإسلام وأمل الأمة القادم .. وستظل باقية بإذن الله

روابط شبكة شموخ الإسلام أعزها الله

الرابط الرقمي | الرابط الرقمي المشفر | الرابط الرقمي 2 | الرابط المباشر | الرابط المباشر المشفر | الرابط المباشر2 | الرابط المباشر المشفر2 |

#1 16-10-2011

أبا عباس القطري
مراقب القسم التقني

المشاركات: 7,553

التحقق من البصمة الرقمية

التحقق من البصمة الرقمية

السلام عليكم و رحمة الله وبركاته

كيف حالكم يا أحبة

كثيرا ما نسمع عن التوقيع الرقمي و غيرها من هذه الأمور

و نسمع عن البصمات الرقمية

و كثيرا ما ندخل مواقع و نجدها تقدم لنا بصمة رقمية

للتحقق من أن الملف هنا يتبع لهذا الموقع

و هي بالعادة تكون عبارة عن مفاتيح من خوارزمية RSA

بطول 2048

المهم

نحن لسنا بصدد معرفة تكوينها أو حتى التعرض لها

لكن كيف من الممكن التحقق من هذه البصمة

و استخدامها

يوجد لدينا برنامجان للتحقق من هذه البصمة

أحدهما gpg4win و الآخر gnupg

تقريبا الاثنان نفس النسخة لكن بإصدارات مختلفة

بجانب كل ملف يوجد له بصمة و عادة ما تنتهي بالامتداد

asc

و لنفترض أن اسم الملف

akalwe.exe

يكون اسم ملف البصمة

akalwe.exe.asc

و لنبدأ بالبرنامج الأول

gpg4win

موقع البرنامج

كود:

```
http://www.gpg4win.org
```

صفحة التحميل

كود:

```
http://www.gpg4win.org/download.html
```

رابط مباشر

كود:

```
http://ftp.gpg4win.org/gpg4win-2.1.0.exe
```

شرح الاستخدام

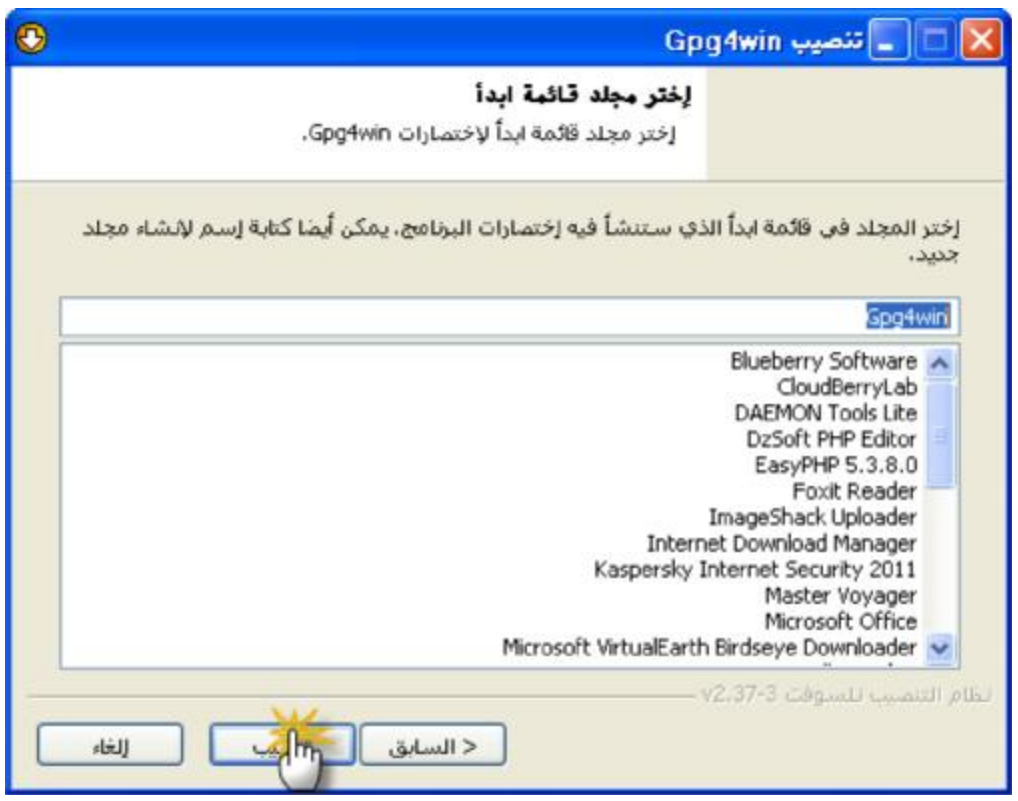

تنصيب Gpg4win
مرحبا في تثبيت Gpg4win
GnuPG هو أداة جنو للاتصالات و التخزين الآمن للبيانات. يُمكن استخدامه لتعمية البيانات و التوقيع الرقمي؛ و هو يشتمل على وسيلة متقدمة لإدارة المفاتيح، ويتوافق مع معيار الإنترنت OpenPGP المقترح كما وُصِف في RFC2440.
إضغط على التالي للمتابعة.
هذه الإصدارة ٢,١,٠ من Gpg4win
إصدارة الملف ٢,١,٠,١٦٤١
تاريخ الإصدار ٢٠١١-٠٣-١٥
إلغاء
التالي >

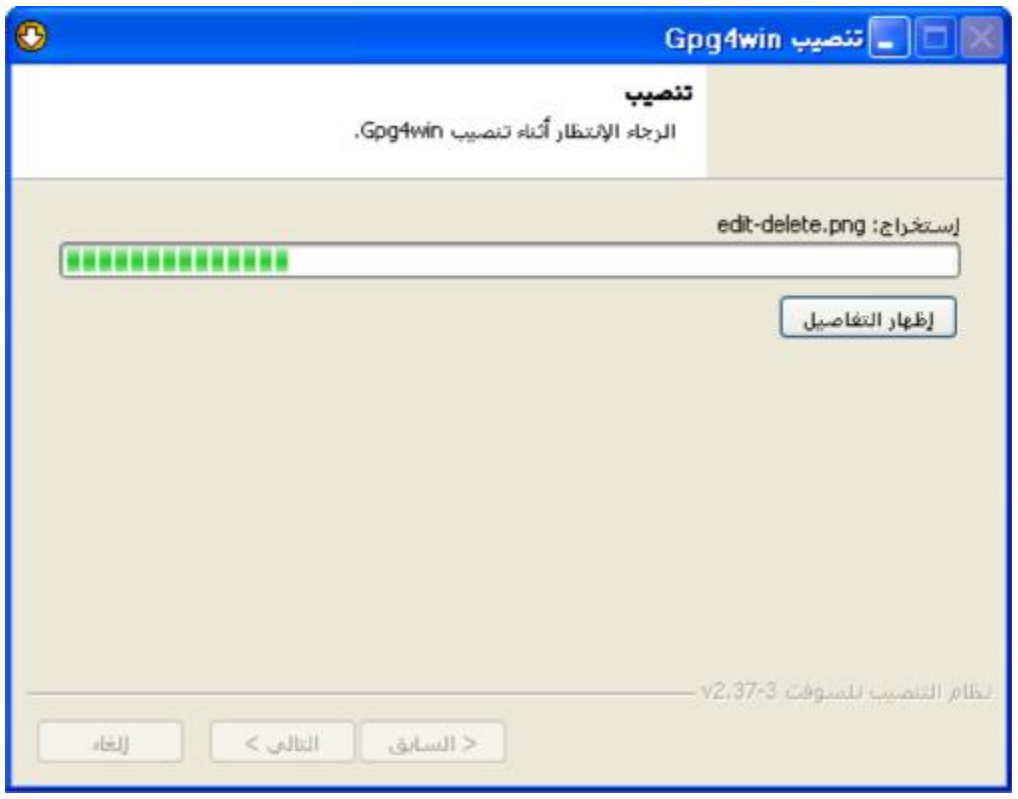

تنصيب Gpg4win
إتفاقية الترخيص
هذه البرمجية مرخصة برخصة جنو العمومية العامة (GPL) والتي تمنحك حرية مشاركة وتعديل البرمجيات الحرة.
إضغط مفتاح صفحة للأسفل لرؤية باقي الإتفاقية
GNU GENERAL PUBLIC LICENSE
Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA ٥١
Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
Preamble
The licenses for most software are designed to take away your
باختصار: تستطيع تشغيل هذه البرمجية لأي غرض. ويمكنك توزيعها ما دمت تعطي المتلقين نفس الحقوق التي حصلت عليها.
نظام التنصيب نلسوفت v2.37-3
إلغاء
التالي >
< السابق

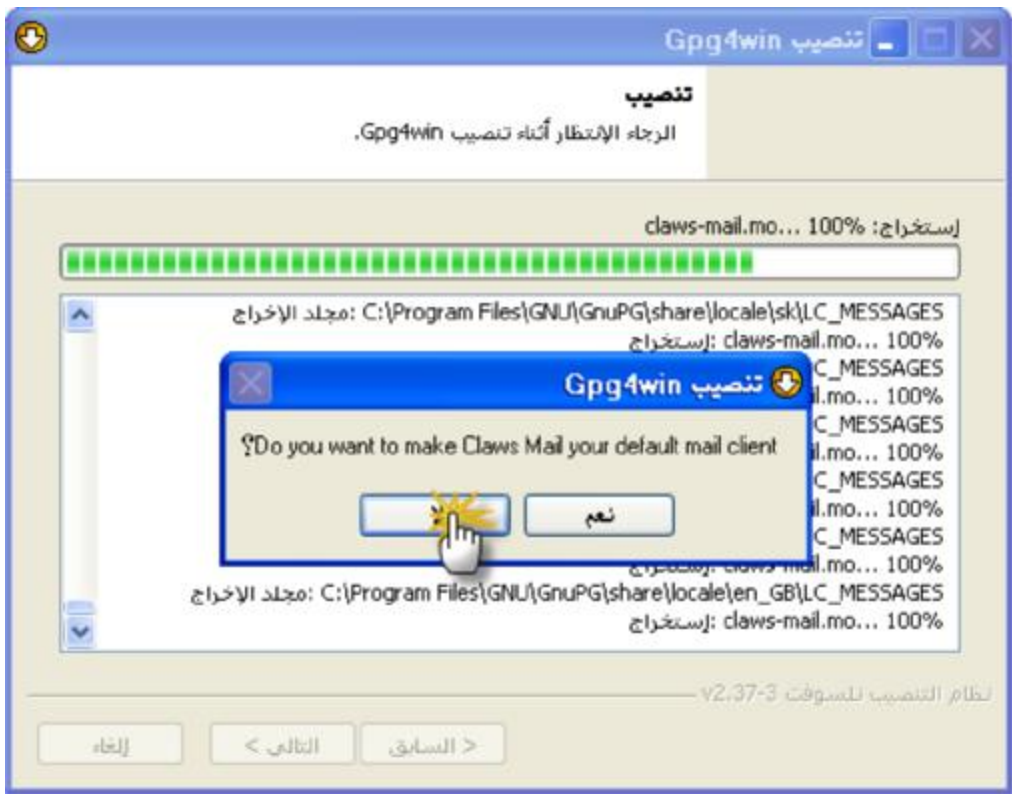

تنصيب Gpg4win
إختر المكونات
إختر ميزات Gpg4win المراد تنصيبها.
حددهم جميعا
علّم المكونات المراد تنصيبها وازل العلامة عن المكونات الغير مراد تنصيبها. إضغط على التالي للمتابعة.
إختر المكونات للتنصيب:
GnuPG
Kleopatra
GPA
GpgOL
GpgEX
Claws-Mail
وثائق Gpg4win
الوصف
برمجية البريد Claws
المساحة المطلوبة:
١٢٢,٥ ميغابايت
نظام التنصيب نلسوفت v2.37-3
إلغاء
التالي >
< السابق

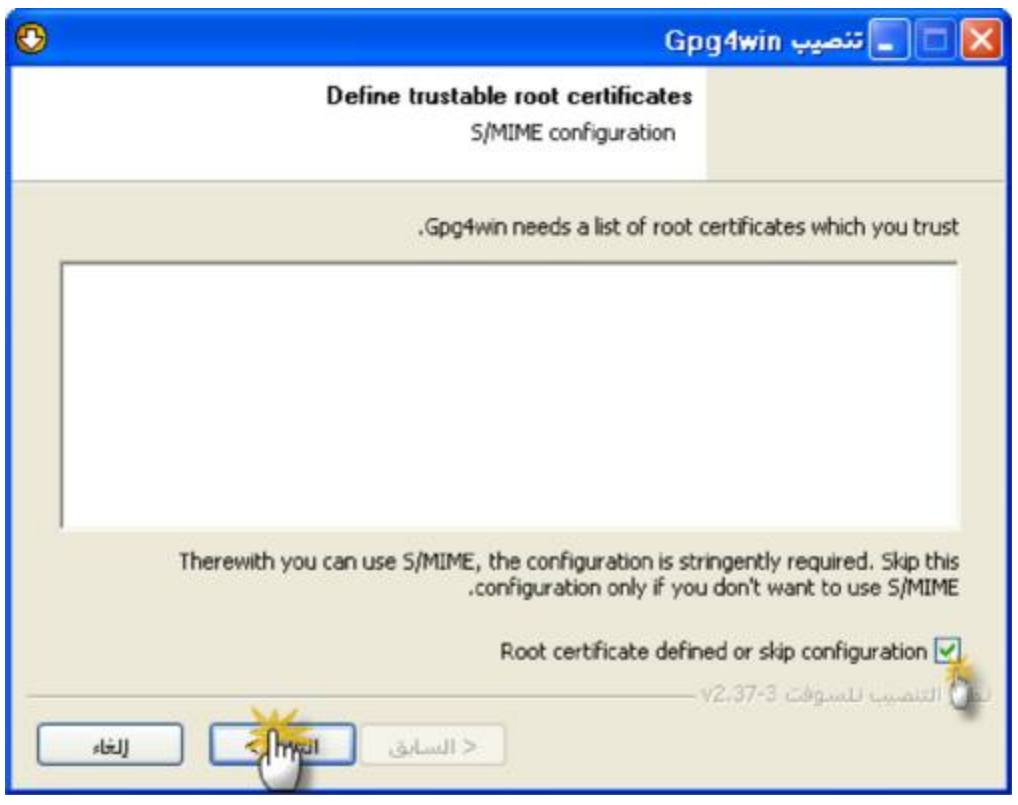

تنصيب Gpg4win
إختر موقع التنصيب
إختر المجلد المراد تنصيب Gpg4win فيه.
سيتم تنصيب Gpg4win في المجلد التالي. للتنصيب في مجلد آخر، إضغط عرض وإختر مجلد آخر.
إضغط على التالي للمتابعة.
مجلد الهدف
عرض...
C:\Program Files\GNU\GnuPG
المساحة المطلوبة: ١٠٢,٥ميغابايت
المساحة المتوفرة: ٨,٩جيغابايت
نظام التنصيب نلسوفت v2.37-3
إلغاء
< السابق


تنصيب Gpg4win
خيارات التثبيت
وصلات البدء
اختر أين يتعين تثبيت الوصلات:
قائمة ابدأ
سطح المكتب
شريط البدء السريع
(فقط البرمجيات سيربط إليها في شريط البدء السريع.)
نظام التنصيب نلسوفت v2.37-3
إلغاء
< السابق

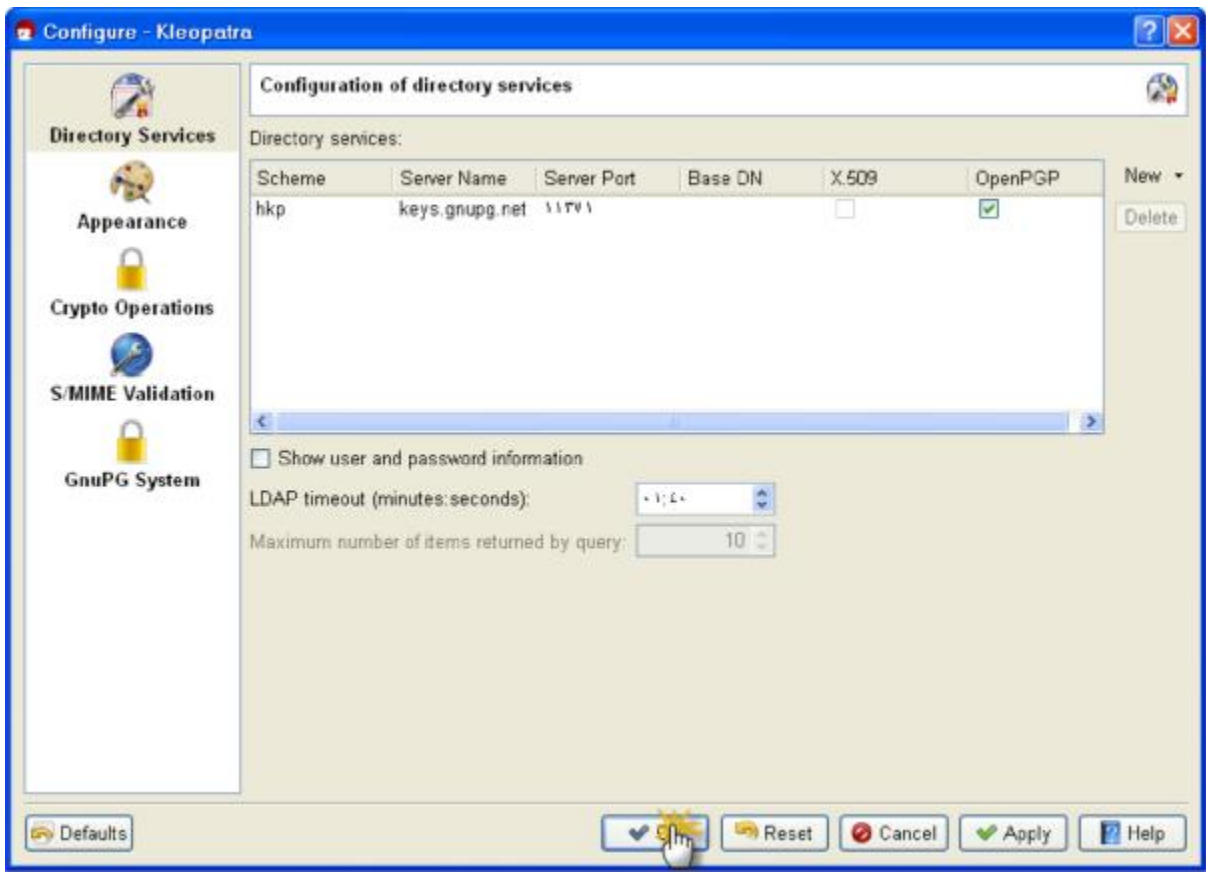

تنصيب Gpg4win
إختر مجلد قائمة ابدأ
إختر مجلد قائمة ابدأ لإختصارات Gpg4win.
إختر المجلد في قائمة ابدأ الذي ستنشأ فيه إختصارات البرنامج. يمكن أيضا كتابة إسم لإنشاء مجلد جديد.
Gpg4win
Blueberry Software
CloudBerryLab
DAEMON Tools Lite
DzSoft PHP Editor
EasyPHP 5.3.8.0
Foxit Reader
ImageShack Uploader
Internet Download Manager
Kaspersky Internet Security 2011
Master Voyager
Microsoft Office
Microsoft VirtualEarth Birdseye Downloader
نظام التنصيب نلسوفت v2.37-3
إلغاء
< السابق

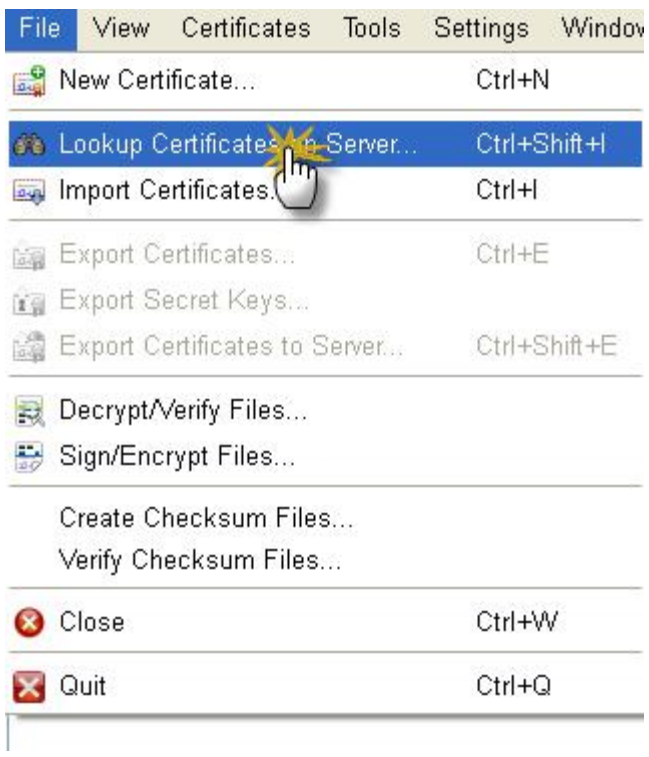

تنصيب Gpg4win
تنصيب
الرجاء الإنتظار أثناء تنصيب Gpg4win.
إستخراج: edit-delete.png
إظهار التفاصيل
نظام التنصيب نلسوفت v2.37-3
إلغاء
التالي >
< السابق


تنصيب Gpg4win
تنصيب
الرجاء الإنتظار أثناء تنصيب Gpg4win.
إستخراج: claws-mail.mo... 100%
مجلد الإخراج: C:\Program Files\GNU\GnuPG\share\locale\sk\LC_MESSAGES
إستخراج: claws-mail.mo... 100%
تنصيب Gpg4win
Do you want to make Claws Mail your default mail client؟
نعم
مجلد الإخراج: C:\Program Files\GNU\GnuPG\share\locale\en_GB\LC_MESSAGES
إستخراج: claws-mail.mo... 100%
نظام التنصيب نلسوفت v2.37-3
إلغاء
التالي >
< السابق


تنصيب Gpg4win
Define trustable root certificates
S/MIME configuration
.Gpg4win needs a list of root certificates which you trust
Therewith you can use S/MIME, the configuration is stringently required. Skip this configuration only if you don't want to use S/MIME.
Root certificate defined or skip configuration
نظام التنصيب نلسوفت v2.37-3
إلغاء
التالي >
< السابق

نقوم بفتح البرنامج





سنأخذ هنا بصمة برنامج التور

التحقق من البصمة يتم عن طريقان

الطريقة الأولى online و الطريقة الثانية offline

و الطريقتان متلازمتان

اسم المفتاح لبرنامج التور يقدمه الموقع

من خلال هذه الصفحة

كود:

```
https://www.torproject.org/docs/signing-keys.html.en
```

بحيث أنه لكل مجموعة من التوزيعات مفتاح

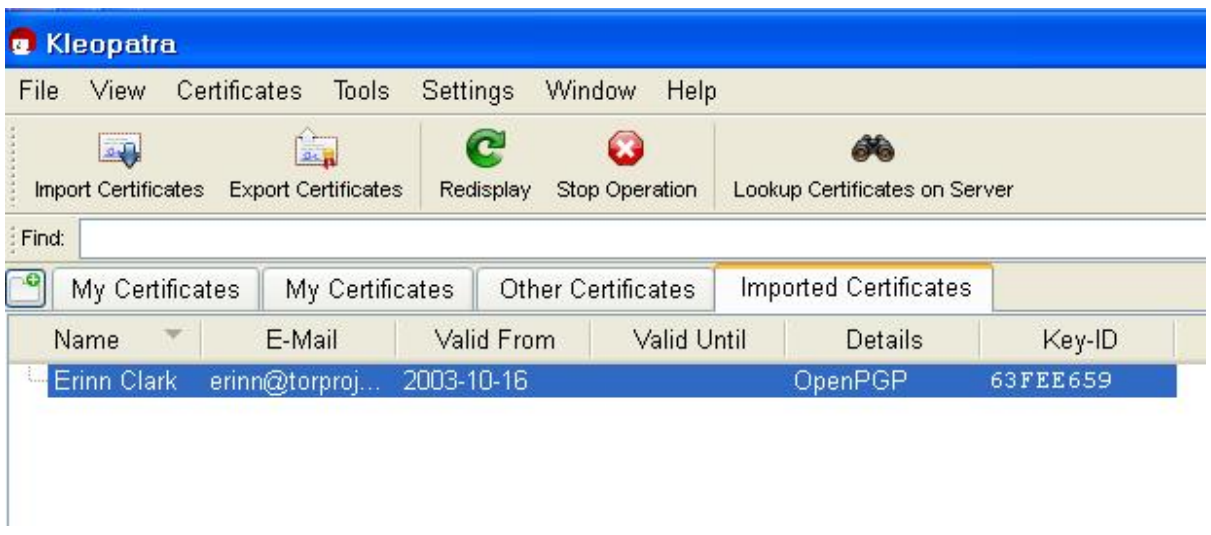
و لنأخذ مثال التور المحمول tor browser

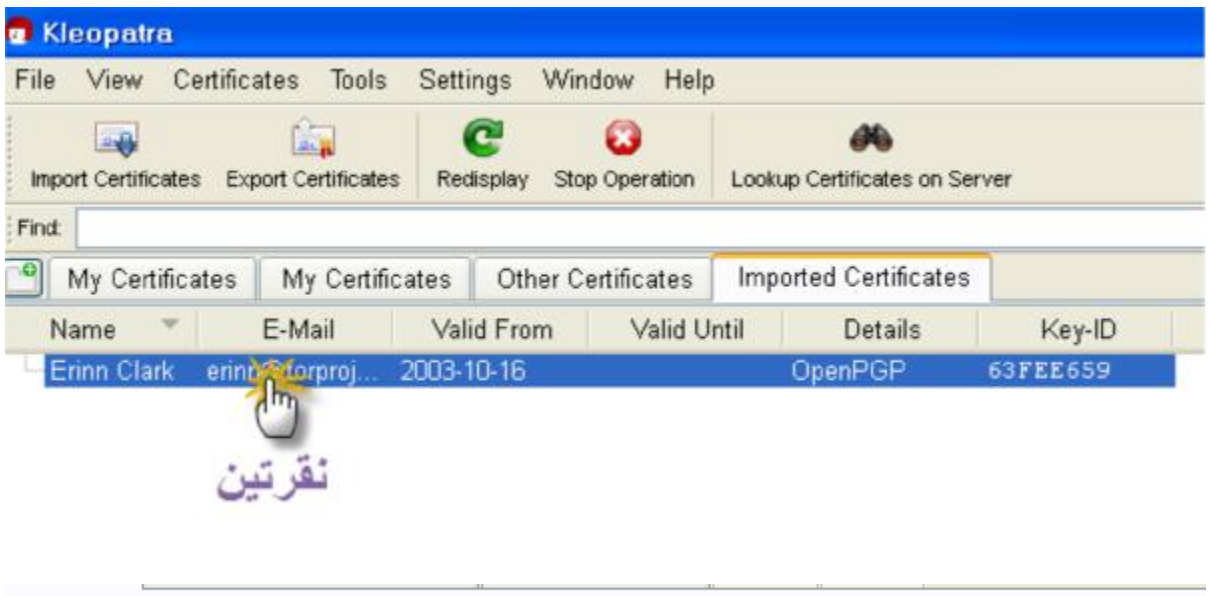
و اسم مفتاحه من الموقع

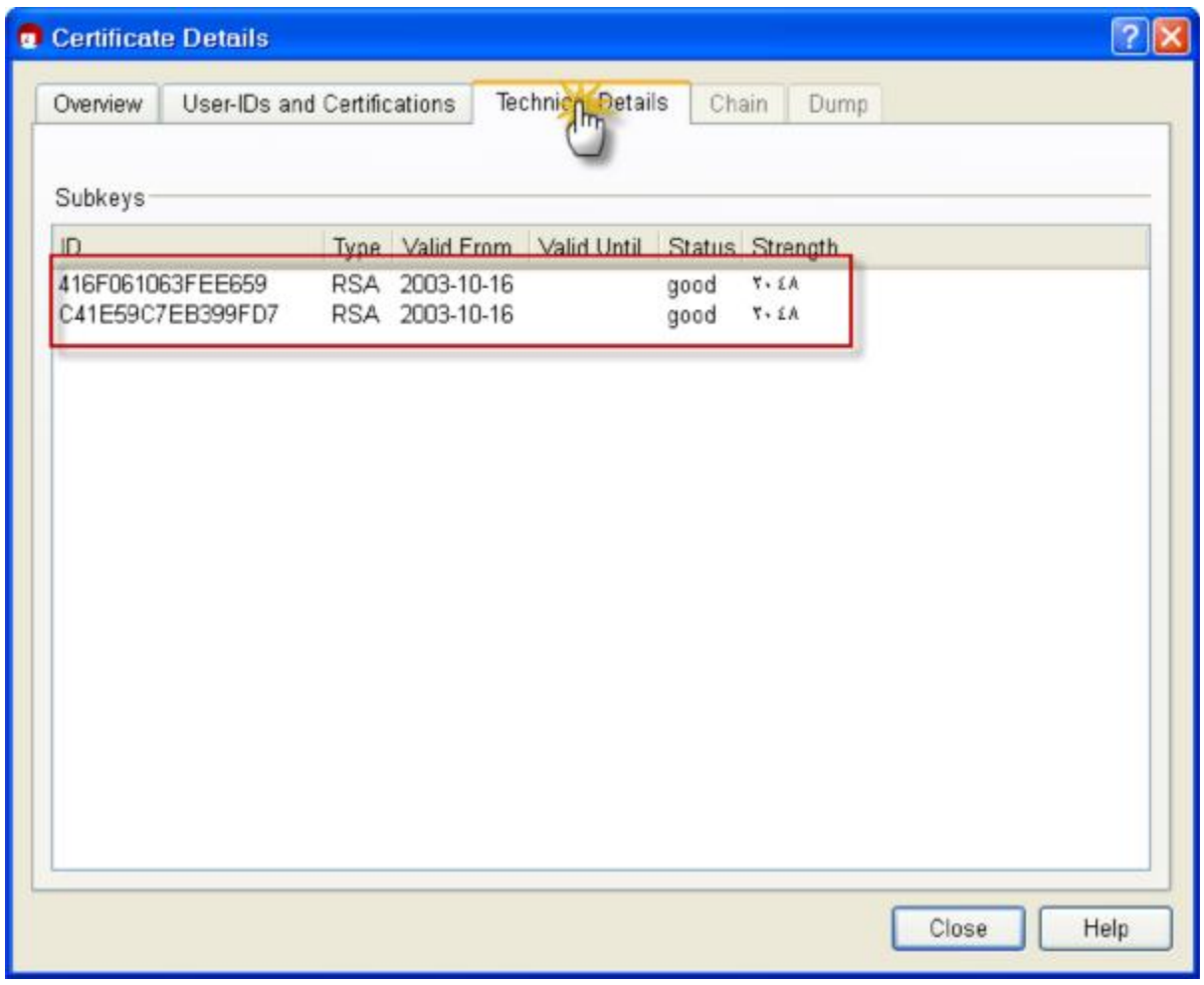
كود:

```
0x63FEE659
```

نقوم بأخذ هذا المفتاح و وضعه في البرنامج







أهم البيانات الموجودة في المفتاح محددة

و هي اسم مالك المفتاح و خوارزمية المفتاح و طولها

و صلاحية المفتاح و finger point

بصمة المفتاح

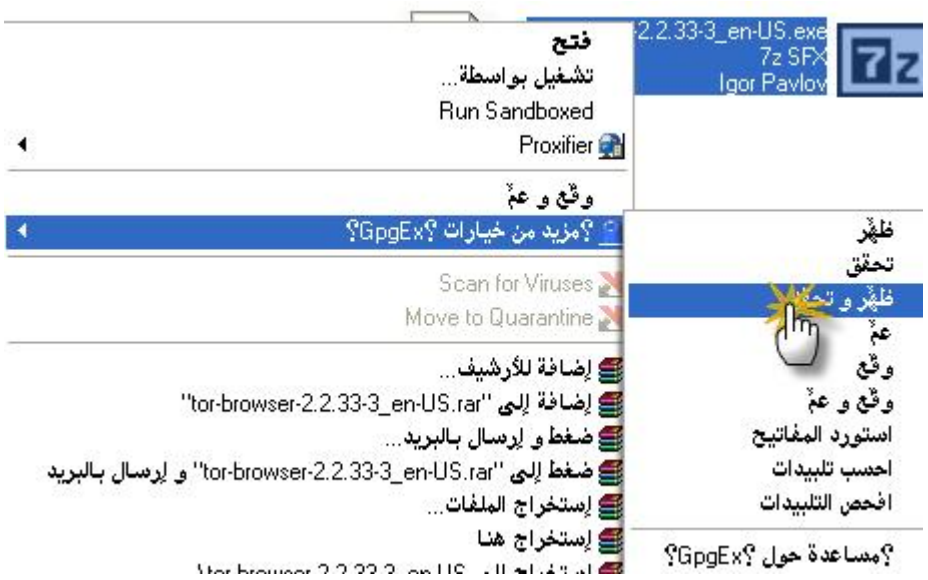
سنقوم بمطابقة هذه البيانات بالبيانات التي لدينا

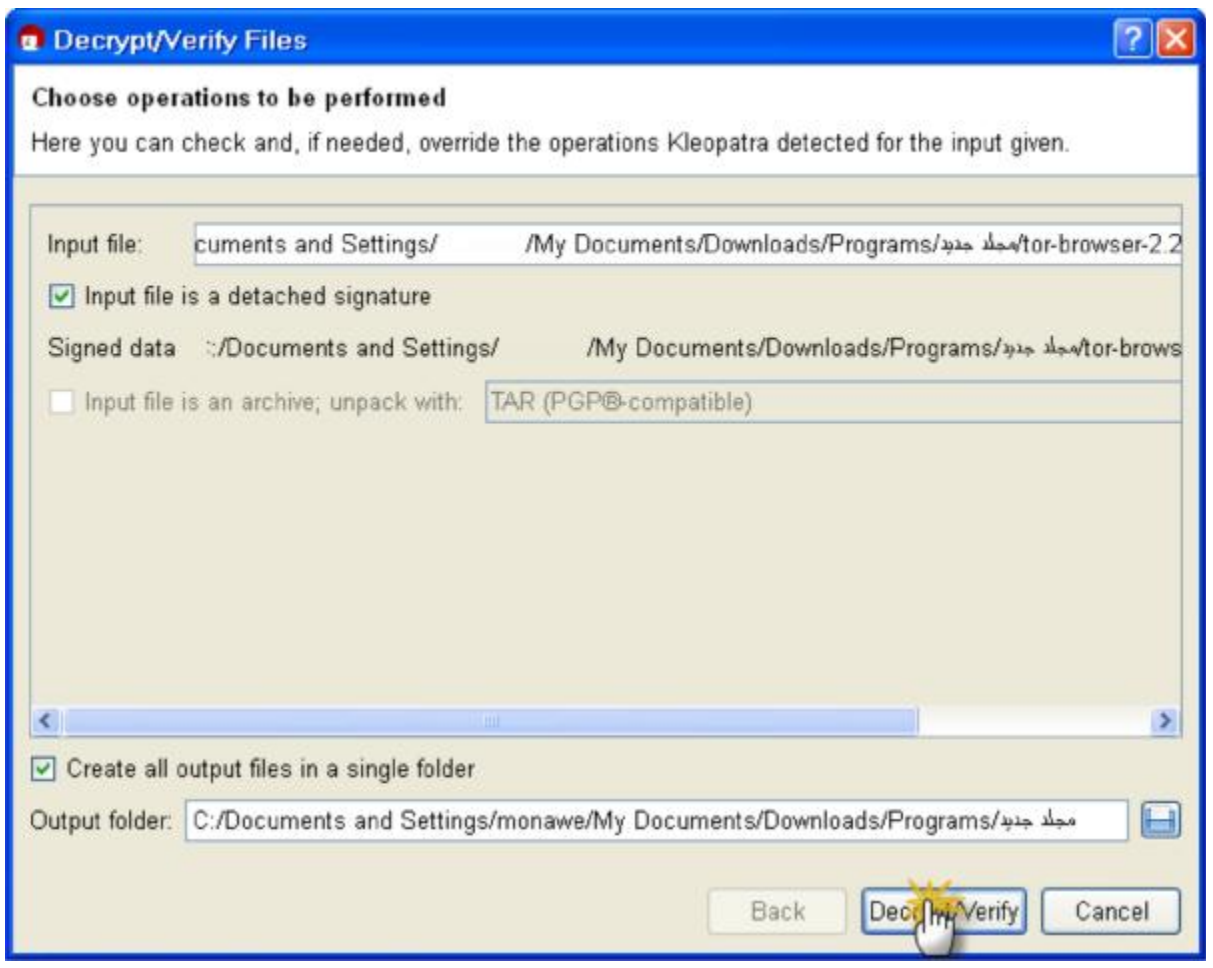
نبقي البرنامج مفتوح

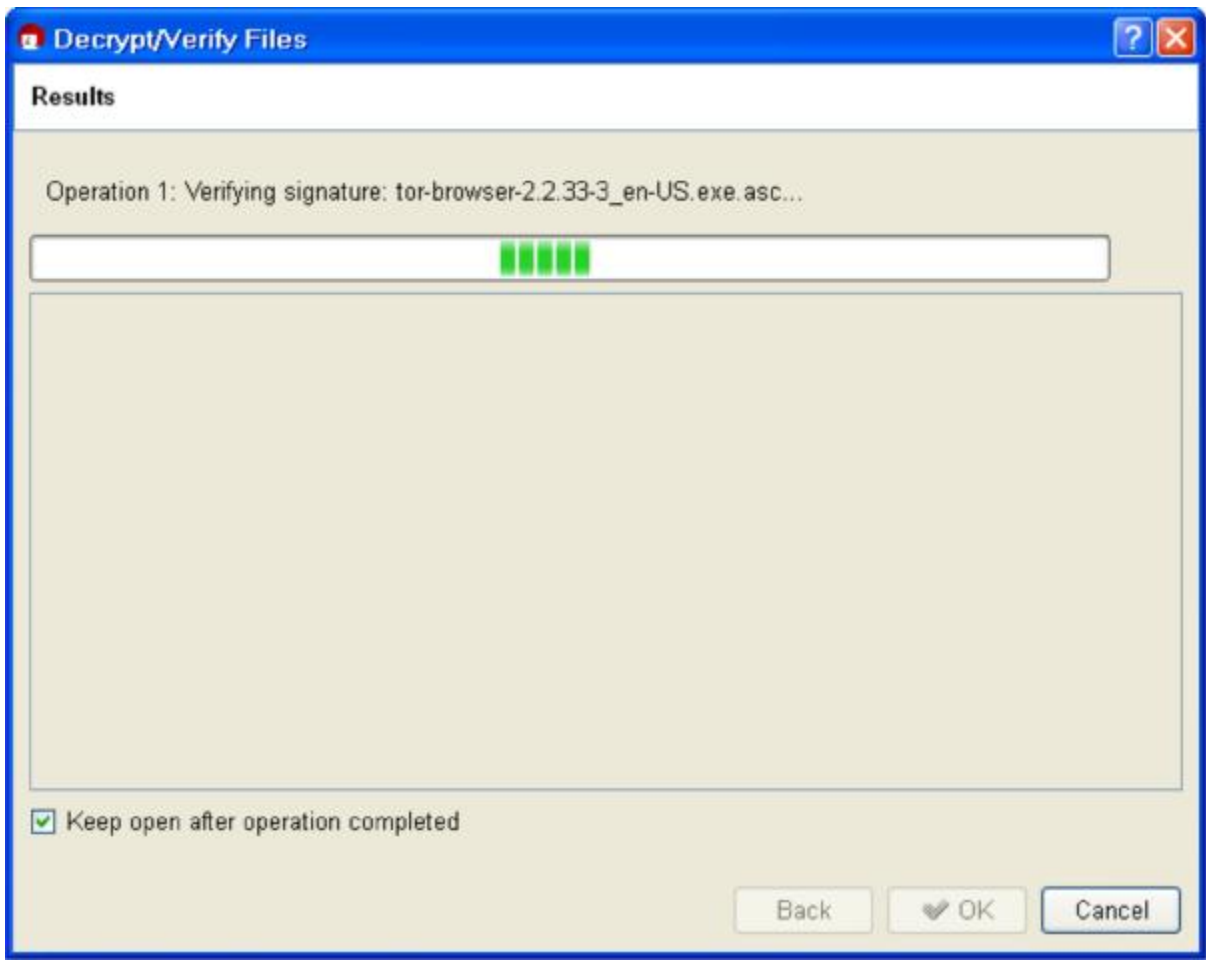
و نقوم بوضع الملف و بصمته في مجلد واحد

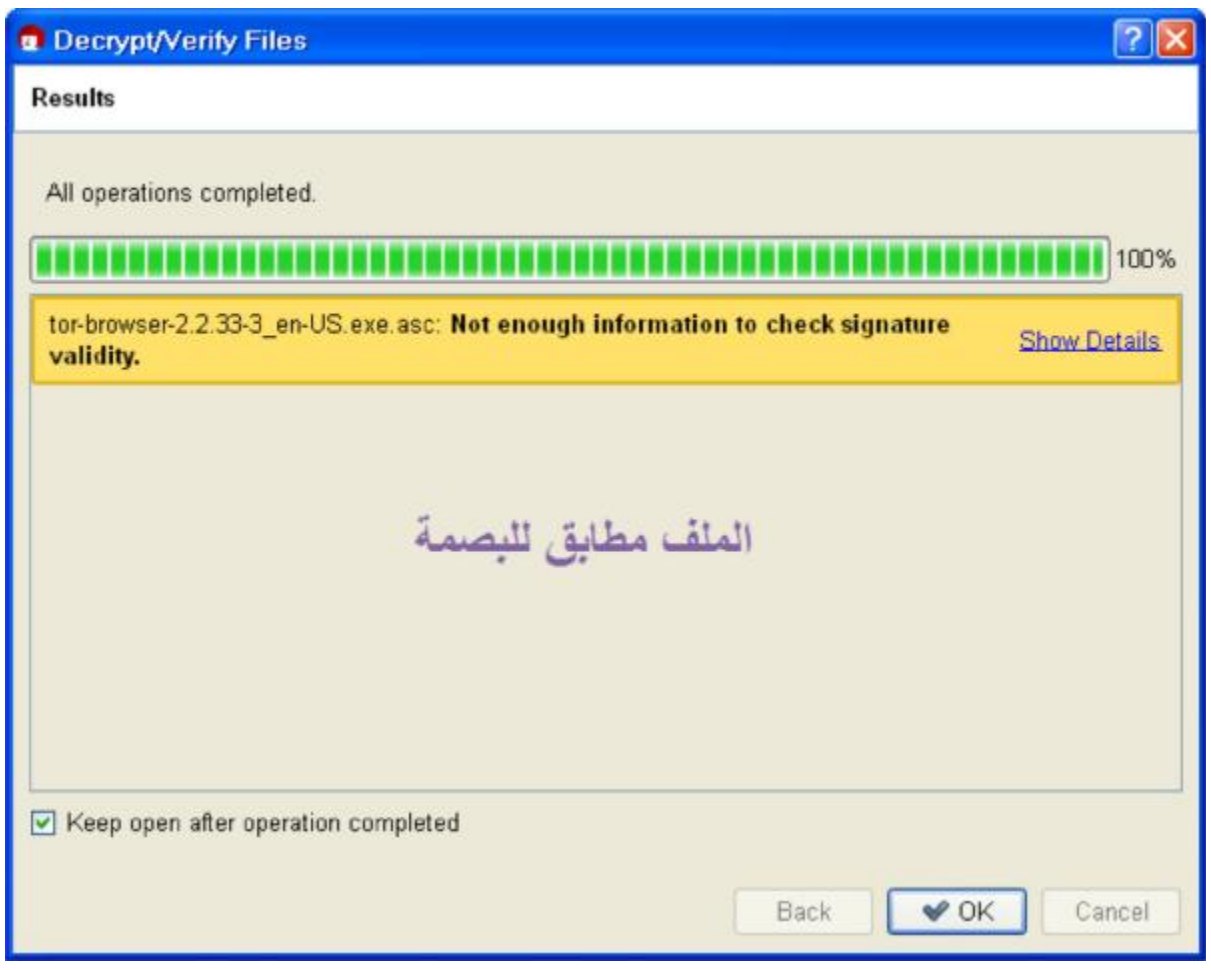
الملف و البصمة في نفس المجلد

نتوجه إلى الملف و نفعل التالي

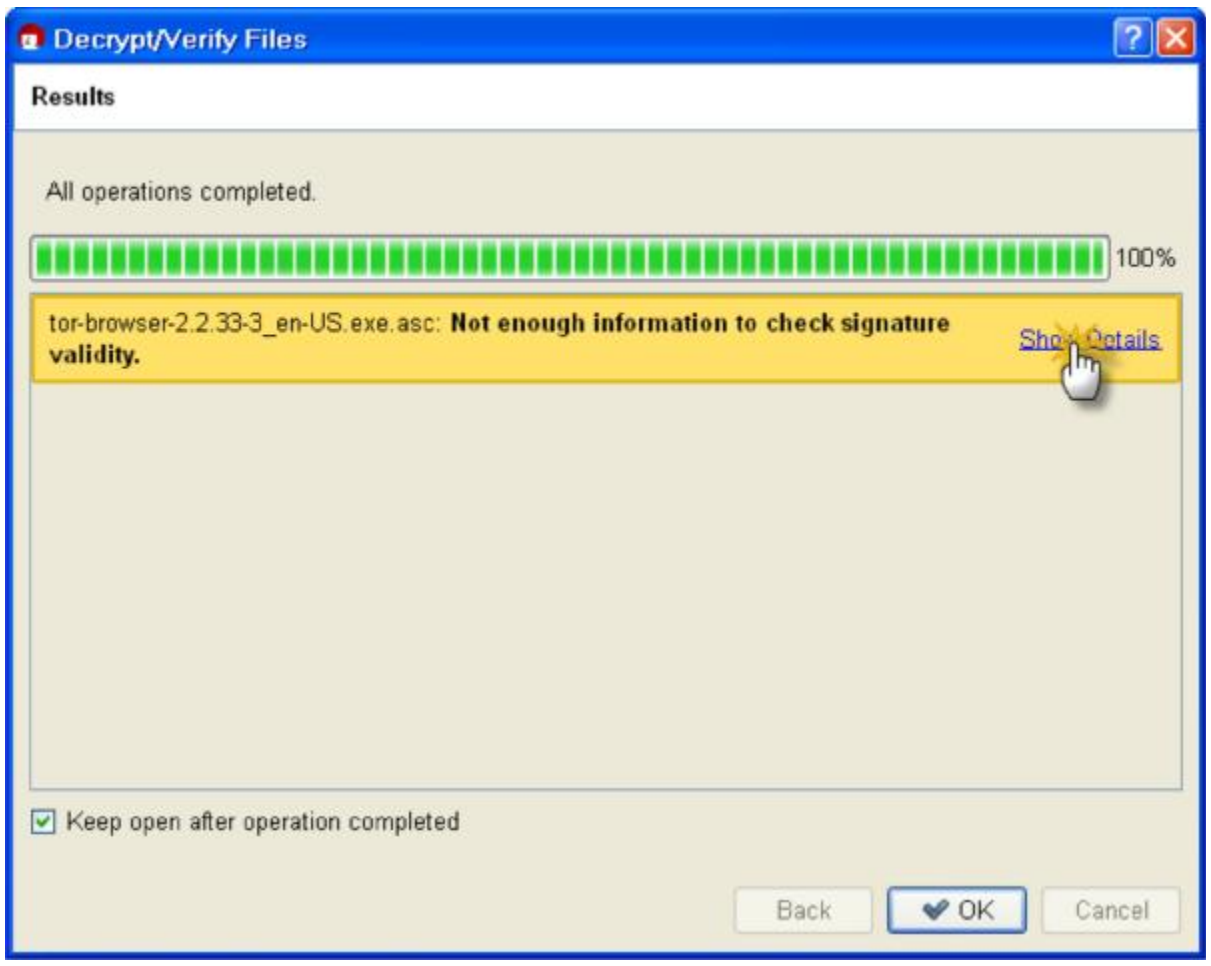


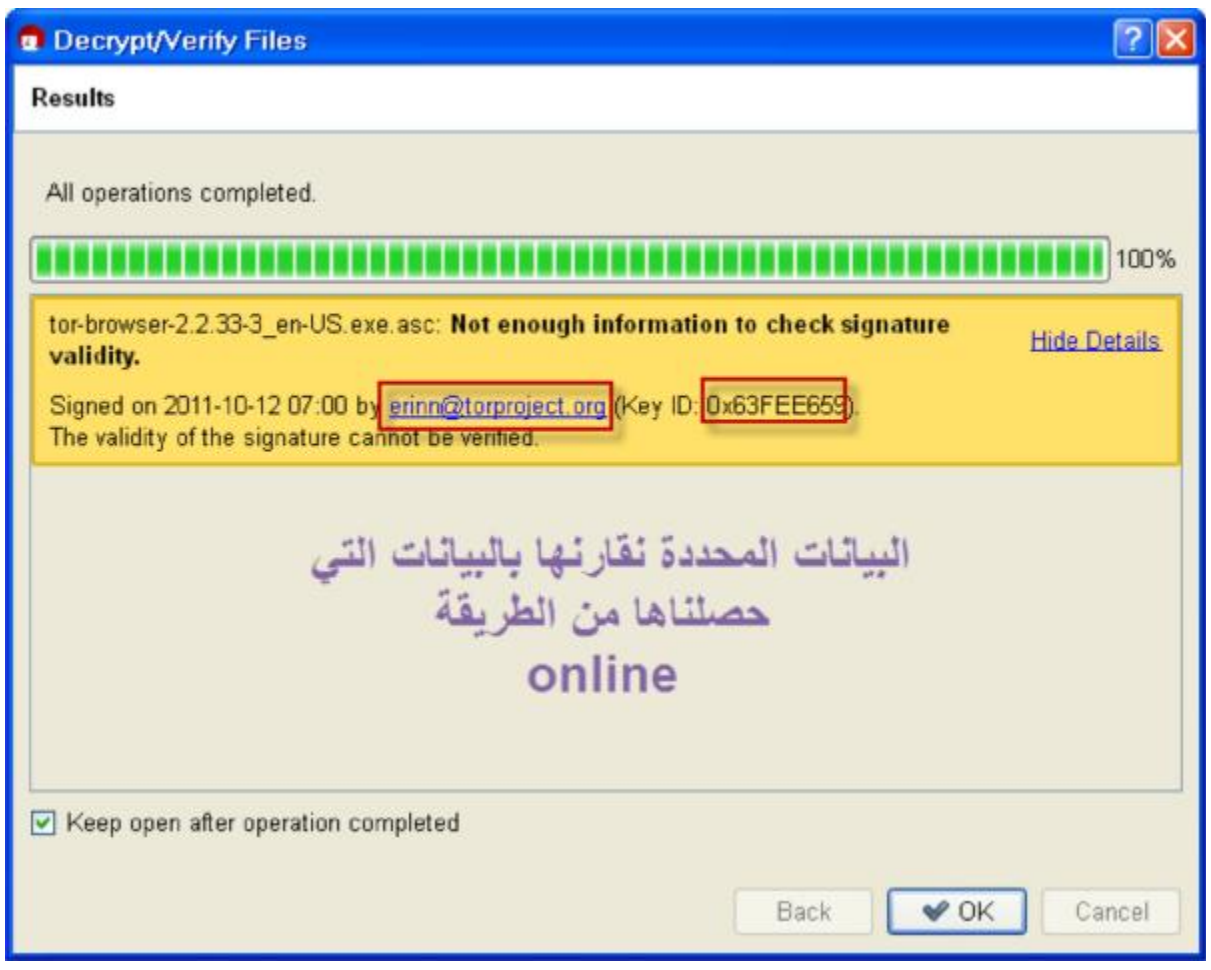






و للتأكد من أن البصمة تتبع المفتاح نقوم بالتالي

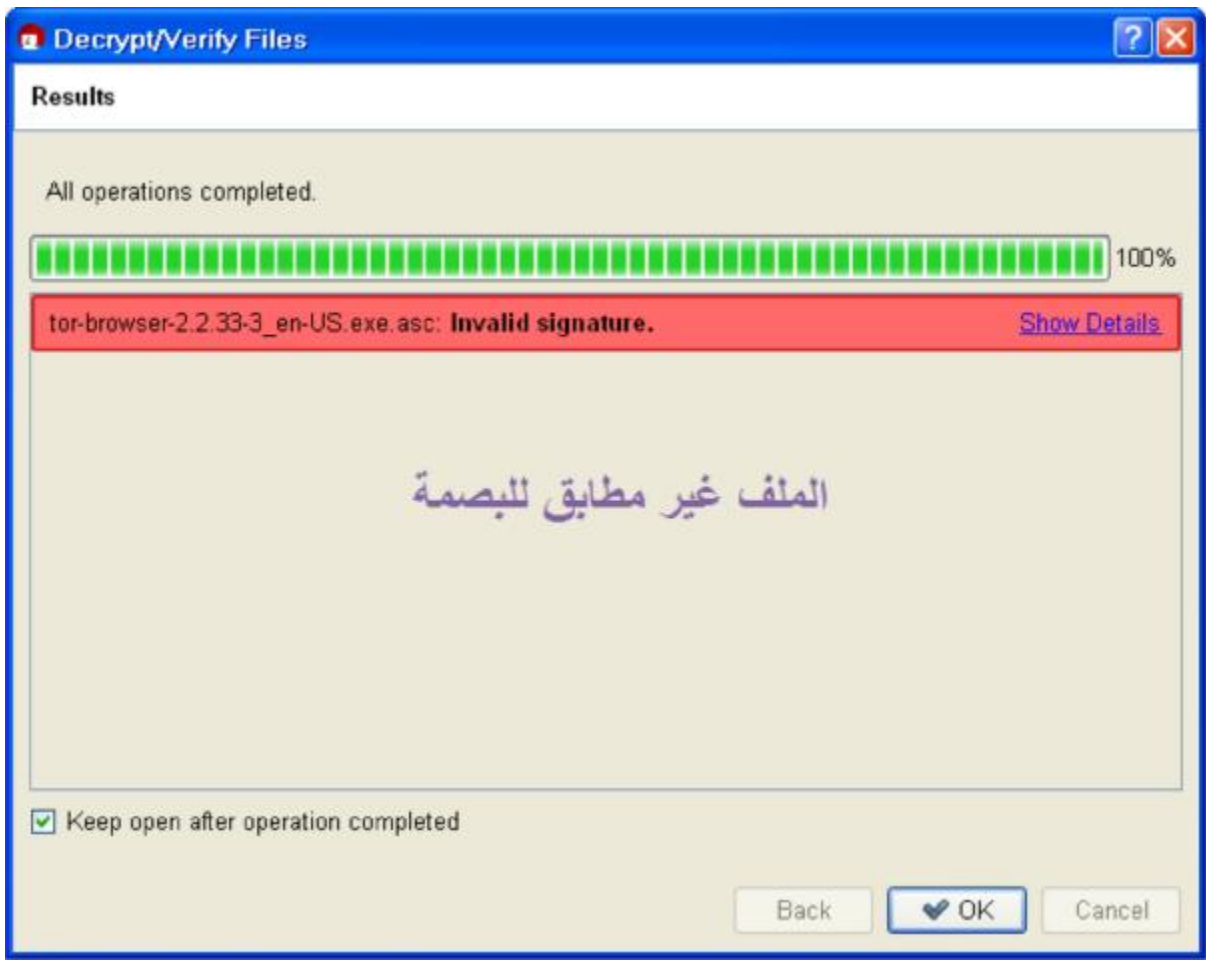




و إذا تطابقت البيانات يكون الملف سليم

لم تتطابق يكون الملف ليس تابع لهذا المفتاح

ظهور هذه الصورة



الملف غير مطابق للبصمة

تعديل المشاركة | إضافة رد | رد مع اقتباس

16-10-2011 #2

أبا عباس القطري
مراقب القسم التقني

المشاركات: 7,553

البرنامج الثاني

و هو أفضل من البرنامج الأول

gnupg

موقع البرنامج

كود:

```
http://www.pgpi.org/
```

صفحة التحميل

كود:

```
ftp://ftp.pgpi.org/pub/pgp/gnupg
```

رابط مباشر

كود:

```
ftp://ftp.pgpi.org/pub/pgp/gnupg/gnupg-w32cli-1.2.2.zip
```

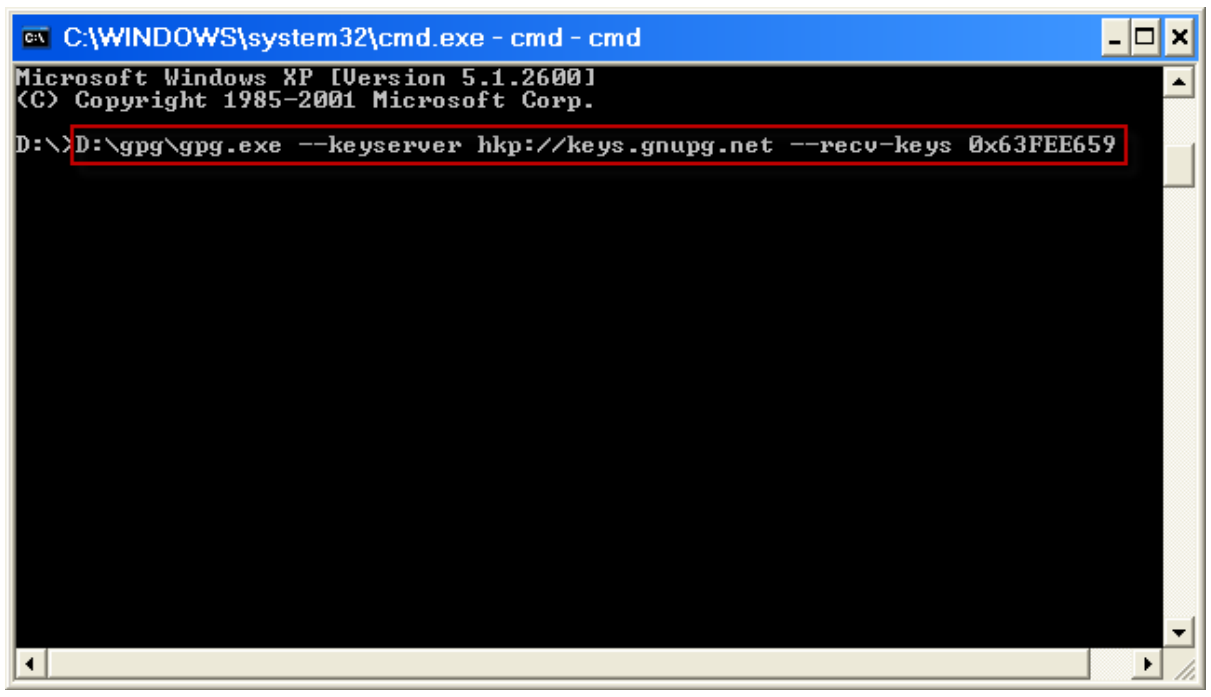
شرح الاستخدام

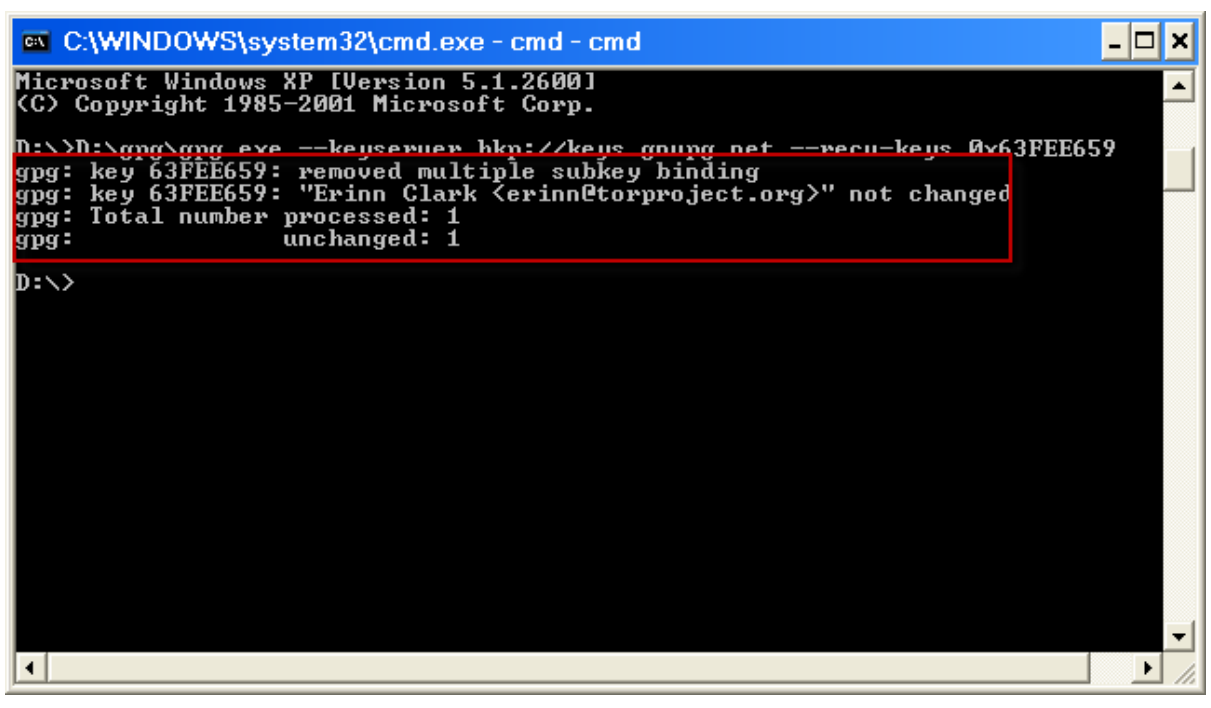
فك الضغط عن الملف

أكتب بجانبه هذه الكلمات

كود:

```
--keyserver hkp://keys.gnupg.net --recv-keys 0x63FEE659
```



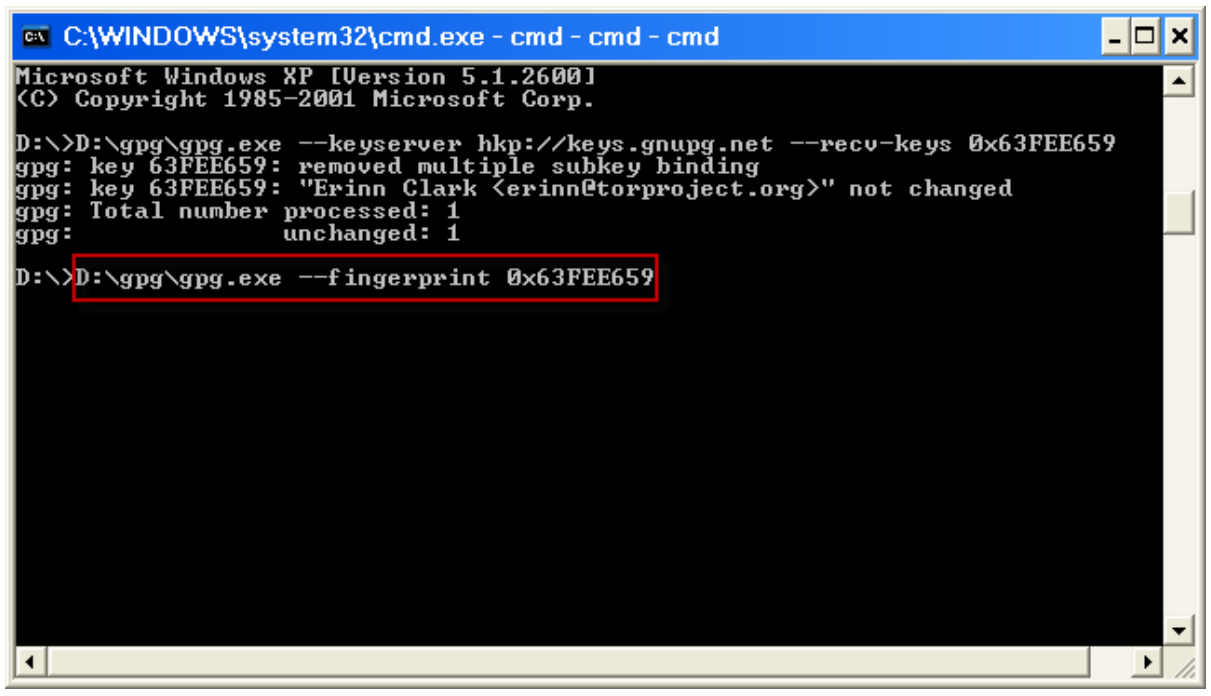


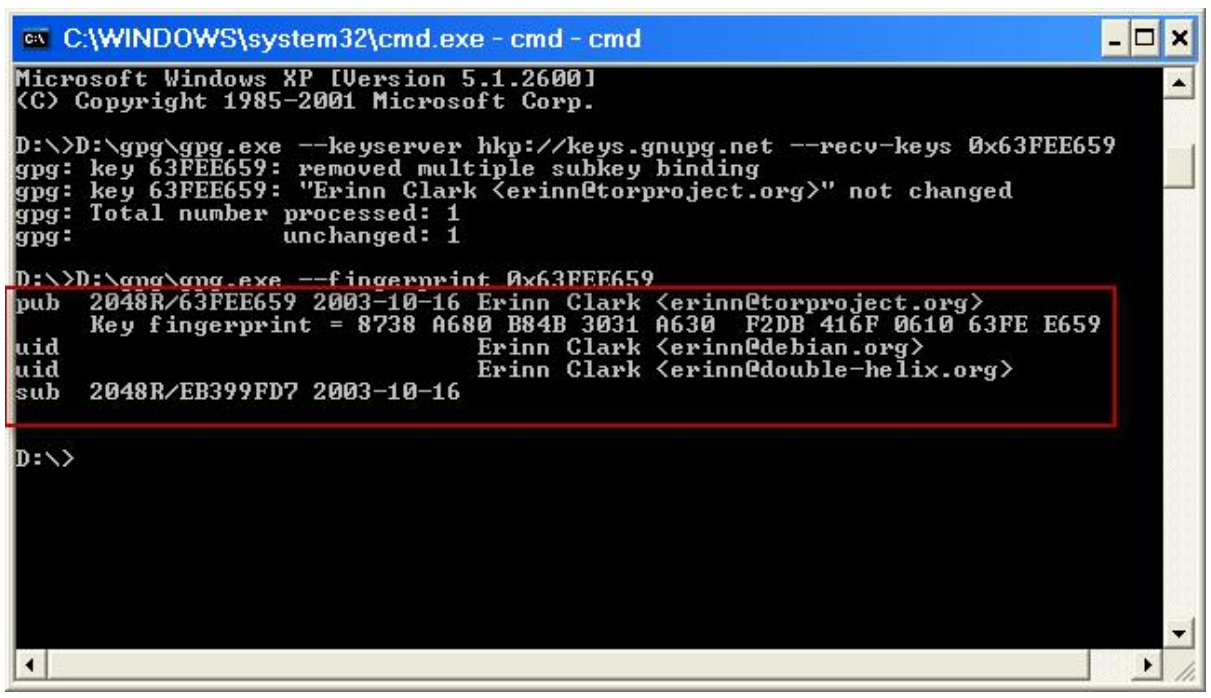
مرة أخرى

نضع هذا الكلام بجانبه

كود:

```
--fingerprint 0x63FEE659
```





ها نحن حصلنا البيانات online

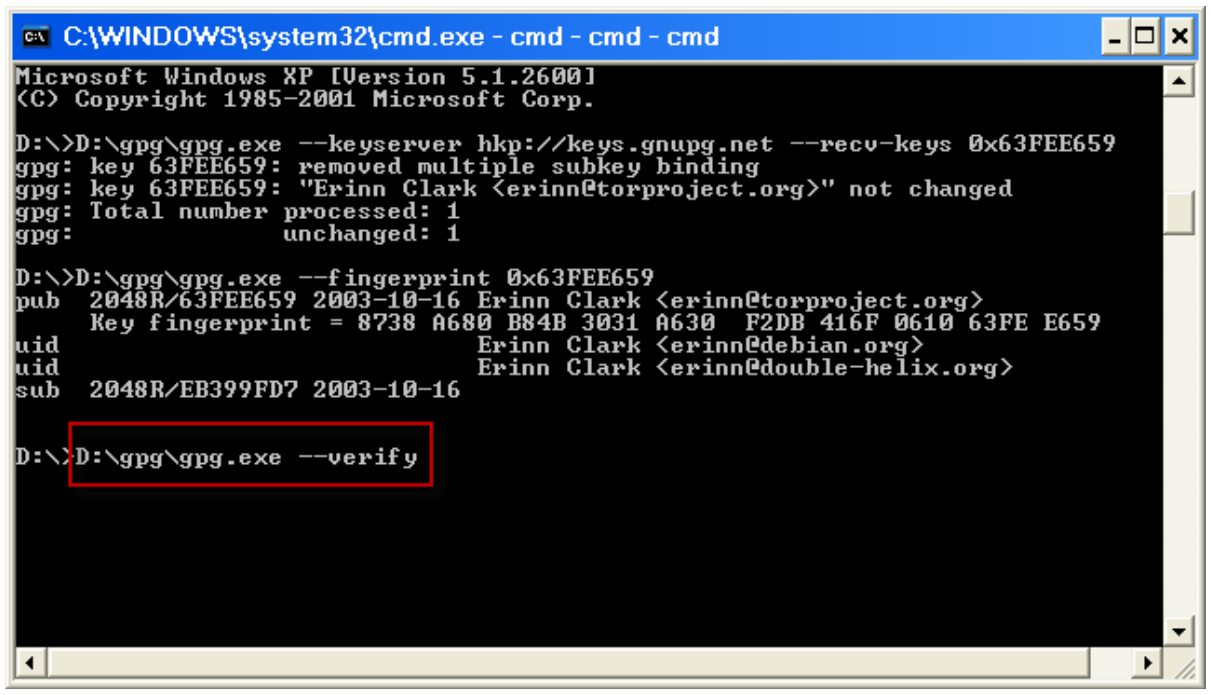
حان الوقت للتحقق

مرة أخرى

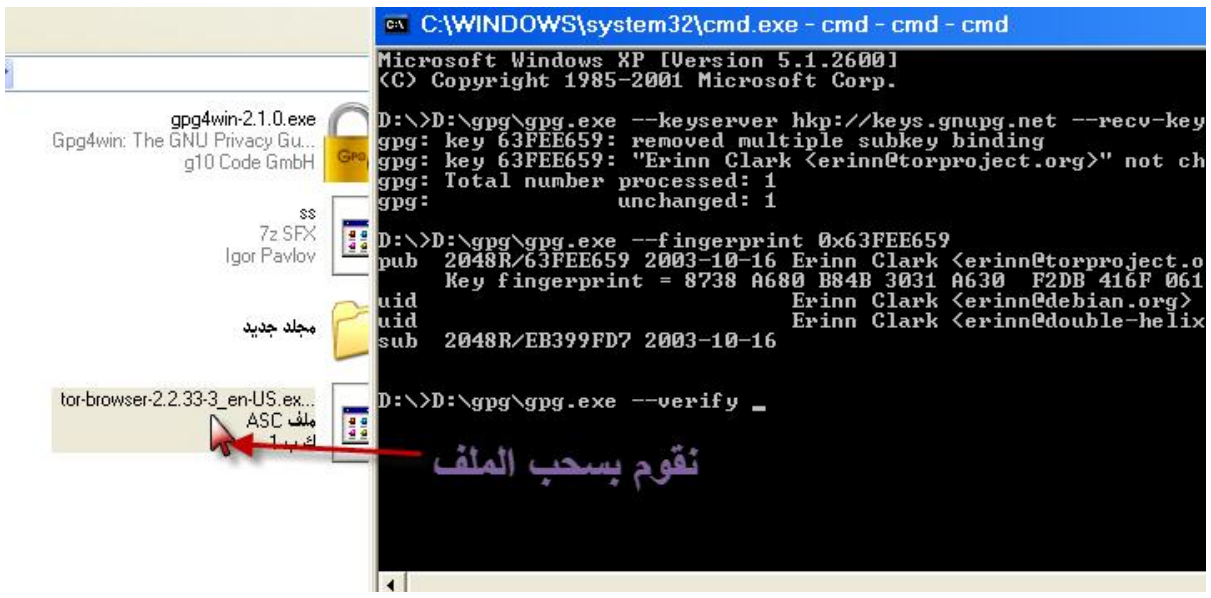
نضع هذا الكلام بجانبه

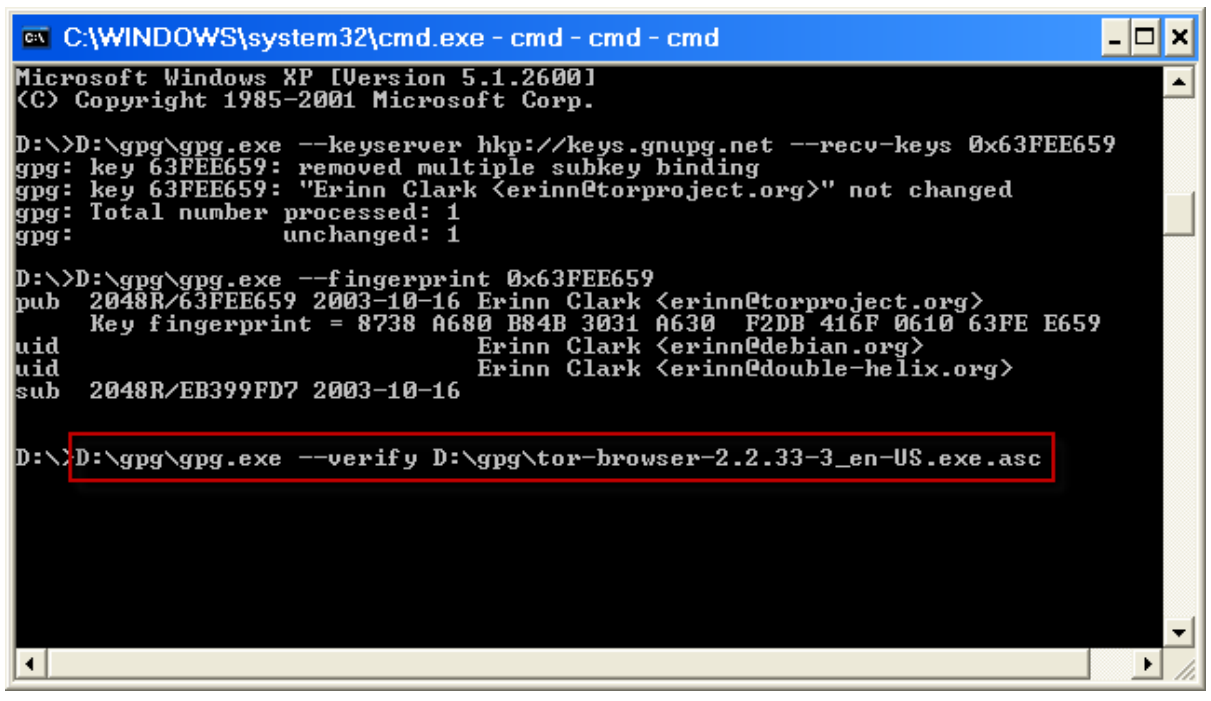
كود:

```
--verify
```



نقوم بسحب ملف البصمة





نقوم بمقارنة البيانات الموجودة الآن بالبيانات من الطريقة online

و كما ترى هناك كلمة good signature

و هي تدل أن هناك تطابق

هنا لا يوجد تطابق و كما نرى هناك كلمة bad signature

و هي تدل أنه لا يوجد تطابق

التعديل الأخير تم بواسطة أبا عباس القطري ; ***2011-10-16*** الساعة ***08:21 AM***

تعديل المشاركة | **إضافة رد** | **رد مع اقتباس**

16-10-2011 #3

أبا عباس القطري
مراقب القسم التقني

المشاركات: 7,553

ملاحظات

ما أود قوله هو أن الطريقة تتلخص كالتالي

التحقق من الملف من عدة مصادر

المصدر الأول هو البصمة الرقمية المرفقة مع الملف

المصدر الثاني هو بيانات المفتاح الموجودة

على موقع خاص بهذا الأمر

المصدر الثالث هو بيانات المفاتيح المرفقة على الموقع نفسه

المفروض هذه الثلاثة مصادر يكون بينها تطابق تام

طريقة التحقق

1- نأتي بالبيانات من الموقع

2- نقارن الملف بالبصمة الرقمية المرفقة

3- نقارن البيانات التي خرجت مع البيانات من الموقع

الثلاث خطوات متلازمات و لا يفترقن

مخالفة خطوة تؤكد أن الملف غير سليم

البرنامج الأول أفضل من الثاني

لأن البرنامج الثاني يقدم معلومات أكثر عند مقارنة الملف

بالبصمة الرقمية

بعكس الأول

الذي يقدم فقط مالك المفتاح و اسمه

أين نجد البصمة

عادة ما تكون بجانب الملف المراد تحميله

كالصورة التالية

التعديل الأخير تم بواسطة أبا عباس القطري ; ***2011-10-16*** الساعة ***AM 08:22***

تعديل المشاركة | إضافة رد | رد مع اقتباس

16-10-2011 #4

أبا عباس القطري
مراقب القسم التقني

المشاركات: 7,553

بالنسبة للإخوة أصحاب أنظمة الماك

بإمكانك استخدام أوامر الطريقة الثانية

مع هذا البرنامج

كود:

```
http://macgpg.sourceforge.net/
```

بالنسبة للإخوة أصحاب أنظمة الديبيان

مراجعة الصفحة التالية

كود:

```
https://www.torproject.org/docs/debian.html.en#packages
```

بالنسبة للإخوة أصحاب أنظمة prms

بواسطة الأمر التالي

كود:

```
rpm -K filename.rpm
```

بالنسبة للإخوة أصحاب أنظمة اللينكس

معظم التوزيعات تأتي معها

gpg preinstalled

كل ما عليه هو استخدام أوامر الماك

لمزيد من المعلومات

راجع الصفحات التالية

كود:

```
https://www.torproject.org/docs/verifying-signatures.html.en
```

كود:

```
https://www.torproject.org/docs/signing-keys.html.en
```

كود:

```
http://http-keys.gnupg.net/
```

كود:

```
http://www.gnupg.org/********ation/
```